REMARKS

Claims 1-31 are pending in this application. Claim 17 is cancelled without prejudice or disclaimer and proposed amendments to claims 26 and 27 are presented herein.

The Examiner's notification of the allowability of claims 2, 11, 19 and 27-31, if rewritten in independent form, is noted with appreciation.

The participation of the Examiner and the Supervisory Examiner in an Examiner Interview on May 24, 2005 is also noted with appreciation.

Claim 26 is amended to incorporate a limitation previously recited in its dependent claim 27. The limitation is accordingly deleted from claim 27.

Claims 17 and 26 stand rejected under 35 USC §102(b) as anticipated by Ganesan (U.S. Patent No. 5,535,276). Claims 1-16, 18-25 and 27-31 stand rejected under 35 USC §103(a) as obvious over Ganesan in view of Spies, et al. (U.S. Patent No. 6,230,269). The rejection is moot with respect to claim 17, in view of its cancellation. The rejection of claims 1-16 and 18-31 is respectfully traversed.

As discussed during the Interview, Ganesan discloses a private key, a first portion of which is a user's password. Thus, Ganesan does not generate the first private key portion or transform messages with a generated first private key portion. Rather, Ganesan applies the password as the first private key portion to transform messages which can be further transformed with the second private key portion and/or public key portion of the asymmetric key.

Spies discloses generating the entire asymmetric key (i.e., the private and public key pair) based upon the user's password. Accordingly, Spies also is incapable of generating only a portion of the full private key based on the user's password.

As discussed during the above-referenced Examiner Interview, claim 1 requires a second processor representing a user that is capable of generating only the first private key portion responsive to receipt of an inputting of and based on the user password. It is respectfully submitted that neither Ganesan nor Spies disclose a processor having such a capability. Accordingly, it is respectfully submitted that there is nothing within the proposed combination to suggest modifying Ganesan such that only the first private key portion is generated based on the user's password.

As also discussed during the Interview, as described in the present specification, the second private key portion of the private crypto-key generated by the first processor of claim 1 is not based on the user password.

Independent claim 9 requires a first processor representing a user, which is capable of generating, based on a user's password, a first portion of a private crypto-key and transforming a message with the first private key portion before destroying the generated private key portion. As discussed above, Ganesan does not generate a first private key portion, but rather applies the password itself as the first private key portion. Spies teaches generating the entire asymmetric crypto-key based on the user's password and lacks any suggestion that only a portion of the private key of a private/public key pair could or should be generated using a password. Indeed, Spies is solely concerned with the public/private key pair, and accordingly fails to even recognize the benefit of generating only one portion of a split private key based on a password.

Independent claim 18 requires generating, based on a user password, a private crypto-key and a corresponding public crypto-key associated with the user, and dividing the private crypto-key into first and second private key portions. Also required is that the private crypto-key and first private key portion be destroyed without distribution or storage in a persistent state. Additionally required is that responsive to receipt of and based upon the user password, only the first private key portion be separately generated. As discussed above, it is respectfully submitted that the combination of Ganesan and Spies fails to suggest such a technique for generating an asymmetric crypto-key or separately generating only the first private key portion based on the user's password.

Claim 26, as amended, requires the processing of a password to generate the first private key portion and transforming a first message with the generated first private key portion. Also required is that the first private key portion not be stored at any network device and not be transmitted over the network. As discussed above, neither Ganesan or Spies suggest the processing of the password to generate a first private key portion which is used to transform a message and which is neither stored at any networked device nor transmitted over the network.

Accordingly, it is respectfully submitted that each of independent claims 1, 9, 18 and 26 patentably distinguish over the applied prior art in that only a portion of the private key is generated based upon the user's password, and in certain of these claims also in that messages are transformed without the private key portion being stored on any network device or transmitted over the network.

As has been discussed in response to a prior Official Action, it is also respectfully submitted that other features recited in the dependent claims further distinguish over the applied prior art. For example, it is believed that those claims requiring selective operation in two modes with a one way function applied a different number of times to generate the first private key portion in each mode, are distinguishable over the applied prior art. Likewise, those claims requiring the selection between different one way functions, based for example on the user's identity or strength of the user's password, and the generation of a private key portion based on the selected function, would also appear to patentably distinguish over the applied prior art.

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed local telephone number, in order to expedite resolution of any remaining issues and further to expedite passage of the application to issue, if any further comments, questions or suggestions arise in connection with the application.

To the extent necessary, Applicants petition for an extension of time under 37 CFR § 1.136. Please charge any shortage in fees due in connection with the filing of

this paper, including extension of time fees, to the Deposit Account No. 01-2135

(Case No. 1160.41369X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Alfred A. Stadnicki
Registration No. 30,226

1300 North Seventeenth Street
Suite 1800
Arlington, VA 22209
Tel.: 703-312-6600
Fax.: 703-312-6666

AAS/slk